Evans, Sandra E

From: SCaldwell@BealBank.com
Sent: Tuesday, October 14, 2003 9:41 AM
To: regs.comments@occ.treas.gov; regs.comments@ots.treas.gov
Subject: FW: FIL comment

8

> -----Original Message-----
> From: Sonya Caldwell
> Sent: Monday, October 13, 2003 4:35 PM
> To: 'comments@fdic.gov'; 'regs.comment@occ.treas.gov';
'regs.comments@federalreserve.gov'; 'regs.comment@ots.treas.gov'
> Subject: FIL comment
>
> October 13, 2003
> Public Information Room
> Office of the Comptroller of the Currency
> 250 E Street, SW, Mailstop 1-5
> Washington, DC 20219
> ATTN: Docket No. 03-18
> Jennifer J. Johnson
> Secretary
> Board of Governors of the Federal Reserve System
> 20th Street and Constitution Avenue, NW
> Washington, DC 20551
> ATTN: Docket No. OP-115
> Robert E. Feldman
> Federal Deposit of Insurance Corporation
> 550 17th Street, NW
> Washington, DC 20429
> Regulation Comments
> Chief Counsel's Office
> Office of Thrift Supervision
> 1700 G Street, NW
> Washington, DC 20552
> ATTN: Docket No. 03-35
> Re: Proposed Interagency Guidance on Response Programs for
Unauthorized Access to Customer Information and Customer Notice
> Dear Sirs or Madams:
> This comment is submitted on behalf of Beal Bank in response to the
Notice and Request for Comment issued by the Federal Deposit Insurance
Corporation, Federal Reserve Board, Office of the Comptroller of the
Currency and Office of Thrift Supervision (collectively, "the Agencies")
regarding the "Interagency Guidance on Response Programs for
Unauthorized Access to Customer Information and Customer Notice"
("Proposed Guidance").
> The proposed guidance fulfills a requirement in section 501 (b) of the
Gramm-Leach-Bliley Act and the Interagency Guidelines Establishing
Standards for Safeguarding Customer Information and describes the
Agencies' expectations regarding the response programs that a financial
institution should develop to protect against and address reasonably
foreseeable risks associated with internal and external threats to the
security of customer information maintained by the financial
institutions or its service provider.
> The Proposed Guidance states that "when a checking, savings, or other
deposit account number, debit, or credit card account number, personal
identification number [PIN], password, or other unique identifier has
been accessed or misused, the financial institution should secure the
account, and all other accounts and bank services that can be accessed
using the same account number or name and password combination until
such time as the financial institution and the customer agree on a
course of action." Given the Proposed Guidance's language, the exact
meaning of "secure accounts," is not clear.

> Does "secure the account" mean to close the account? Or does "secure" mean an action that blocks its use in all situations, such as a "freeze?" Although the bank is not opposed to securing the account, we suggest that accounts should only be closed when the risk of fraud is imminent and only after the customer has been notified. Requiring that all accounts be closed in all instances will place unnecessary burden on the customer with the time spent transferring account activity. We also suggest that accounts be "secured" at the discretion of the financial institution and the customer.
> Clarification on this component of the response system would be greatly appreciated. If you have any questions regarding the matters discussed in this comment, please do not hesitate to contact us.
> Thank you.
> Sincerely,
> Molly Curl, SVP Compliance
> Beal Bank - Plano, Texas
>
>
>